Wolfe, S.E., Higgins, G.E., & Marcum, C.D. (2008). Deterrence and digital piracy: A preliminary examination of the role of viruses. ***Social Science Computer Review,*** 26(3): 317-333. Published by Sage (ISSN: 0894-4393) doi: 10.1177/0894439307309465

Deterrence and Digital Piracy: A Preliminary Examination of the Role of Viruses

Scott E. Wolfe, George E. Higgins, and Catherine D. Marcum

ABSTRACT

Digital piracy has been shown to be an emerging societal problem. However, research has demonstrated limited techniques that effectively combat digital piracy. The purpose of the present study is to examine the utility of computer viruses in deterring digital piracy. The findings from responses to a survey of college students revealed that fear of computer viruses may influence respondents' intentions to engage in digital piracy. The policy implications of this finding are discussed.

The widespread use of personal computers has created new opportunities for criminal activity. One of the most pervasive forms of computer crime is digital piracy (Gopal, Sanders, Bhattacharjee, Agrawal, & Wagner, 2004). Digital piracy is defined as the illegal act of copying digital goods, software, digital documents, digital audio (including music and voice), and digital video for any reason other than to back up without explicit permission from and compensation to the copyright holder (Gopal et al., 2004; Higgins, Fell, & Wilson, 2006). The Internet has facilitated an increase in digital piracy in recent years. Wall (2005) notes four characteristics of the Internet that have enabled individuals to easily commit criminal activity: It allows anonymous communication, it is transnational, it has created a shift in thinking from the ownership of physical property to the ownership of ideas, and it is relatively easy. Additionally, Wall (2005) contends that the Internet facilitates piracy because it allows the offense to take place detached from the copyright holder, which provides the offender with the perception that the act is victimless.

Several researchers have acknowledged subforms of digital piracy (i.e., audio and video piracy) as being increasingly pervasive (Gopal et al., 2004; Hinduja, 2003). Higgins et al. (2006) defined audio and video piracy as the "illegal act of uploading or downloading digital sound or video without explicit permission from and compensation to the copyright holder" (p. 4). Technological advancements are partly responsible for the increased ease and accessibility of digital piracy. The International Federation of Phonographic Industries (IFPI, 2006) estimates that one in three music discs purchased around the world is an illegal copy. The IFPI further estimates that 37% of all CDs purchased in 2005 were pirated, resulting in 1.2 billion illegal copies purchased worldwide. In fact, the IFPI concludes that pirate CD sales outnumbered legitimate CD sales in 30 markets across the world and resulted in a loss of $4.5 billion from the music industry.

Digital piracy is a criminal act (Higgins et al., 2006). Mass copyright violations of movies and music were made a felony offense in 1982 by *The Piracy and Counterfeiting Amendments Act*. Additionally, distribution of copyrighted materials over the Internet was made a felony offense by *The No Electronic Theft Act* (Koen & Im, 1997). To date, little research has examined from a criminological perspective the factors that may reduce instances of digital piracy and the individual propensities that attract individuals to digital piracy. Only one study, Higgins et al. (2006), has examined both of these factors within the same study.

Using criminological theory to examine digital piracy is important for two reasons. First, criminological theories allow researchers to organize their empirical data in a rational way. Second, criminological theories provide researchers with potential information for developing policies that can help to reduce instances of digital piracy. Thus, deterrence and selfcontrol theories are attractive because they both focus on the decision-making process for digital piracy. Furthermore, these two theories provide a distinct understanding of the factors that can be used to reduce the instances of digital piracy. In addition, this study uses viruses as an additional deterrent factor that can provide an advance to deterrence theory. This study is important because it will identify the individual propensity (i.e., low selfcontrol) that may reduce an individual's ability to see the inhibiting factors of engaging in digital piracy. Furthermore, it will identify the factors that may reduce the instances of digital piracy. The study begins by outlining deterrence theory and its application to digital piracy through the empirical literature. Next, the study presents low self-control and its relation to digital piracy as seen in the empirical literature. The methods and results follow. The study ends with a discussion that outlines policy implications.

DETERRENCE

The criminal justice system has traditionally relied on deterrence theory to combat crime in the United States. To gain compliance to the law, the criminal justice system seeks out individuals who perform criminal actions and applies punishment to these acts (Tyler & Huo, 2002). The threat of punishment keeps individuals from committing crimes. These forms of deterrence come in two types—specific and general. Specific deterrence occurs when punishment for the commission of an offense prevents or deters the individual from committing the same offense in the future because of fear of further ramifications. General deterrence occurs when individuals not engaging in criminal behavior witness the penalties incurred by another individual that has committed a criminal offense. These people are deterred from committing the particular criminal offense out of fear of receiving the same punishment as the individual that committed the act.

There are two forms of deterrence theory—classical and contemporary. Under classical deterrence theory, humans are assumed to be rational actors. In other words, individuals will elect to perform behaviors that are more pleasurable or beneficial to them than those that are painful or costly. Three factors determine whether an individual will be deterred from committing a criminal act. The certainty (i.e., the individual's belief that the act will be detected), severity (i.e., the individual's belief that the act will be punished severely), and swiftness (i.e., the individual's belief that the act will be detected quickly) must all be high. According to classical deterrence theory, the cost or pain associated with the commission of a criminal act is increased when the threat of detection and punishment are certain, severe, and swift.

The literature has not completely supported the contentions made by classical deterrence theory. Most important, the empirical research has consistently shown that the threat of certainty is more important than severity (Paternoster, 1987; Yu & Liska, 1993). These findings were discovered through meta-analyses of perceptual research that utilized scenarios of criminal activities. Other researchers have found results that support those of these meta-analyses (Grasmick & Bursik, 1990; Nagin, 1998; Nagin & Paternoster, 1991; Piquero & Pogarsky, 2002; Pogarsky, 2002). Because there has not been full support for all concepts of classical deterrence theory, a modern version of the theory has emerged to repair the problems.

Contemporary deterrence theory modified classical deterrence theory by incorporating inhibition and motivation measures for crime. Inclusion of measures such as shame, guilt, and embarrassment were suggested by Grasmick and Bursik (1990) to fully understand how individuals may be deterred from committing criminal acts. Research has shown guilt to be an effective measure that reduces the likelihood of criminal behavior (Nagin & Pogarsky, 2003, 2004; Pogarsky, 2002, 2004). According to Grasmick and Bursik (1990), guilt is a self-stigmatizing measure that acts as an inhibitor to criminal behavior.
An individual's moralistic view of behavior has been considered as an inhibiting factor for deterrence theory as well. Bachman, Paternoster, and Ward (1992) argued that a belief will act as an inhibiting factor if an individual believes a behavior to be morally wrong. A review of the deterrence literature yields strong support for this contention and shows that moral beliefs are an important factor in the decision-making process of individuals (Paternoster, 1987; Paternoster & Simpson, 1996; Piquero & Tibbetts, 1996; Pogarsky 2002, 2004; Tibbetts, 1997). Research of software piracy has shown that individuals are more likely to engage in this behavior when they believe it to be moral as opposed to immoral (Higgins, 2005; Wagner & Sanders, 2001). A meta-analysis of software piracy

found that a person's moral beliefs and attitudes impact his or her likelihood of engaging in illegal piracy on the computer (Liang & Yan, 2005).

Social disapproval has been argued to be an important inhibiting factor for criminal behavior (Grasmick & Bursik, 1990). Grasmick and Bursik suggested that the possibility of friends and family discovering criminal behavior would function as a form of punishment that could vary in both certainty and severity. The actor could become embarrassed if those that he or she admires, trusts, or is close to become aware of participation in a criminal act. Pogarsky (2002) showed that this contention is correct and that when an individual anticipates this form of discovery and embarrassment, he or she is more likely to be inhibited or deterred from performing the criminal act. Research on software piracy has shown that family disapproval has a significant impact on deterring the behavior by creating a social stigma that, in turn, produced greater inhibitions.

Deterrence literature has also examined the role of previous behavior on future behavior. Research has shown that individuals who had performed a behavior in the past were more likely to engage in the behavior in the future (Nagin & Paternoster, 1991). The researchers concluded that this occurred as a result of past behavior reducing inhibitions on future behavior. Other researchers have found similar findings (Cochran, Wood, Sellers, Wilkerson, & Chamlin, 1998; Nagin & Pogarsky, 2003, 2004; Paternoster, 1986; Paternoster & Piquero, 1995). Past software piracy has also been shown to predict future software piracy (Higgins & Makin, 2004a, 2004b; Higgins, Wilson, & Fell, 2005).

Low self-control (Gottfredson & Hirschi, 1990) has been shown to be a contributing factor in the commission of criminal behavior. Gottfredson and Hirschi define low selfcontrol as the inability of an individual to resist a temptation toward criminal behavior when an opportunity for it exists. An individual with low self-control prefers behaviors that are risky, impulsive, easy, nonempathetic, and immediately gratifying (Gottfredson & Hirschi, 1990). Criminological research has supported the contention that low self-control can lead to criminal behavior (Nagin & Paternoster, 1993; Piquero & Tibbetts, 1996; Tibbetts, 1997; Tibbetts & Myers, 1999). Several studies have shown that low self-control is especially useful in predicting software piracy (Higgins, 2005; Higgins & Makin, 2004a, 2004b; Higgins et al., 2005). Accordingly, this theoretical orientation should be taken into account when examining digital piracy from a deterrence perspective.

Social learning theory (Akers, 1998; Sutherland, 1947) has been shown to be a viable contributor to deterrence research. Specifically, Akers (1998) showed that criminal or deviant peer associations increased an individual's likelihood of engaging in criminal behavior. This perspective has been examined by deterrence researchers, who found that there is a connection between peer association and intention to drink (Pogarsky, 2002). Peer associations have also been shown to be useful predictors of software piracy (Christensen & Eining, 1991; Higgins & Makin, 2004b; Skinner & Fream, 1997).

Sherizen (1995) examined whether or not computer crime can be deterred and concluded that there is a great need for criminologists to examine this behavior using a deterrence perspective. Although researchers have studied the applicability of deterrence theory in explaining software piracy (Gopal & Sanders, 1997; Higgins & Makin, 2004a, 2004b; Higgins et al., 2005; Peace, Galletta, & Thong, 2003), very little deterrence research has examined music piracy. Several researchers that did examine similar topics found that magnitude of consequence and peer perceptions were important variables influencing an individual's decision to pirate music (Chiou, Huang, & Lee, 2005; d'Astous, Colbert, &

Montpetit, 2005). Additional researchers have found that stricter regulations on how music is sold and shared over the Internet would reduce the incidence of music piracy (Easley, Michel, & Devaraj, 2003; Fivelsdal, 2005; Wade, 2004).

The growth in computer use has ushered increased concerns of computer viruses throughout the world (Balthrop, Forrest, Newman, & Williamson, 2004). “The term virus refers to malicious software that requires help from computer users to spread to other computers” (Balthrop et al., 2004, p. 527). Computer viruses can halt essential operations in business, disrupt banking transactions, delay airline flights, and bring down emergency call centers (Balthrop et al.). Although antivirus software is available to computer users, it has been shown that “viruses can spread even when infection probabilities are vanishingly small” (Lloyd & May, 2001, p. 1316). Additionally, it has been demonstrated that “current antivirus and network intrusion detection solutions can become overwhelmed by the burden of capturing and classifying new viral strains and intrusion patterns” (Harmer, Williams, Gunsch, & Lamont, 2002, p. 252). Although such viruses as “Sobig” have caused more than $30 billion in damage across the world (Balthrop et al.), the threat to personal computer users is real and potentially devastating (Balthrop et al.; Harmer et al., 2002; Lloyd & May, 2001). In 2002, it was estimated that there were more than 55,000 different computer virus strains identified (Harmer et al., 2002).

The threat of computer virus infection is omnipresent and potentially unavoidable to users of systems such as music file sharing networks (Balthrop et al., 2004; Harmer et al., 2002; Lloyd & May, 2001). According to reports by the IFPI (2006), individuals who participate in music piracy have fears of contracting a computer virus as a result of the behavior. Most important, it was shown by research analysts “Jupiter” that 35% of a sample had stopped or reduced their music piracy as a direct result of the effects of viruses on computers (IFPI, 2006). This suggests that the threat and potential consequences of viruses deterred individuals in this sample from participating in music piracy. Despite the availability of antivirus software, some music pirates still perceive the risk of computer viruses to be greater than the rewards of the behavior. Additionally, the results suggest that viruses exhibited a certain, severe, and swift consequence of engaging in music piracy that was great enough to deter some individuals. The present study expects to find similar results. Specifically, those individuals that list computer viruses as a potential consequence of engaging in music piracy will be less likely to have intentions to pirate music. The present study is the first known analysis with the purpose of investigating the applicability of deterrence theory on music piracy. Specifically, it is the first study to explicitly examine the deterrent impact of computer viruses on music piracy involvement and behavior. Thus, a gap will be filled in the criminological literature concerning digital piracy. This compelling study will go beyond software piracy literature by examining the role of deterrence theory and computer viruses in music piracy.

THE PRESENT STUDY

The purpose of the present study is to examine the roles of deterrence theory, peer associations, and self-control theory in the context of music piracy. Specifically, this study explores the utility of computer viruses as a deterrent to music piracy. Going beyond Higgins et al. (2006), we expect that contemporary deterrent factors and viruses will have a deterrent effect on digital piracy. The present study adds to the current literature on deterrence theory and expands on it by integrating new deterrent possibilities. Besides important contributions to academia, the present study has provided policy implications for law

enforcement, Internet service providers, and college administrators that can be utilized to combat future music piracy.

METHOD

Procedures and Sampling

This study used a self-report questionnaire administered to college students at several universities in the southeastern United States. On Institutional Review Board and Human Subject Protection review, data were collected during the 2006 fall semester. The survey was handed out to required general education courses open to all majors and courses only open to justice administration majors. Professors of the surveyed classes had given prior permission for the study to take place during class. Students present in class on the day that the questionnaire was administered took part in the study. A cover sheet on the front of the survey explained the purpose of the study, the voluntary nature of the study, and that response would be completely anonymous and confidential. The researchers also verbally stressed these rights to the students as the survey was being handed out. Following these procedures, approximately 400 surveys were collected as part of the sample. Table 1 presents the demographic profile of the sample broken down by sex, race, age, major, and income level. The median age of the sample was 21 years, with a range from 18 to over 25; 39.9% of the sample was male (*n* = 143) and 59.2% were female (*n* = 212); 28.2% of respondents were non-White (*n* = 101), and the remaining 66.2% were White (*n* = 237).

Table 1
Demographic Profile of the Sample

Measure	*F*	%
Sex		
Male	143	39.9
Female	212	59.2
Race/ethnicity		
White	237	66.2
Non-White	101	28.2
Age: Mean = 21 years		
Major		
Business administration	19	5.3
Justice administration	84	23.5
English	3	0.8
Mathematics	7	2.0
Other	239	66.8
Approximate family income in previous year		
0 to $19,999	41	11.5
$20,000 to $29,999	38	10.6
$30,000 to $39,999	48	13.4
$40,000 to $49,999	47	13.1
$50,000 or more	170	47.5

The present study uses a nonrandom sample that can be criticized for lack of generalizability. However, the two theories in question, deterrence and self-control, are considered general theories because they attempt to explain all crime all of the time, no matter the sample. Consequently, a nonrandom sample can be utilized to generalize about a larger population (Love, 2006).

Wright, Caspi, Moffitt, and Paternoster (2004) have criticized researchers for using samples of college students in analyses of deterrence theory, arguing that students may not be likely to engage in the types of criminal behaviors that are being studied. However, the research shows that college students, as a group, are the most likely to engage in digital piracy (Higgins et al., 2006; Hinduja 2001, 2003; Hollinger, 1988; Husted, 2000). College students have regular access to computers, are seen as less grounded in ethical standards, and are less controlled by vigorous rule enforcement on campuses (Hinduja, 2003). Additionally, college students are more likely to engage in digital piracy because they have insufficient financial funds to acquire the products through legitimate means. Therefore, the current study has sampled those individuals most likely to engage in digital piracy.

DESIGN

The present study utilized scenarios on the questionnaire to capture the certainty and severity of consequences following the behavior displayed in the hypothetical situation (Klepper & Nagin, 1989). Important to the study was the development of scenarios that would be believable to the targeted population. After reviewing the literature regarding the measures of deterrence (i.e., certainty and severity), the researchers developed the measures for the present study by administering a 30-item semistructured pilot study survey. This pilot study was given to a sample of approximately 60 college students (the target population) that were excluded from the study sample. With the survey, the researchers were attempting to discern two ideas: (1) the believability of the hypothetical scenarios and (2) the extralegal sanctions of performing the actions in the scenarios. Students were presented with 10 scenarios and were asked to rate the believability of each on an 11-point scale ranging from *not believable* to *100% believable*.

The most believable scenarios were chosen from the pilot study to be included in the administered survey. We chose to use the scenario that 95% of the respondents marked as believable. The scenario involving the type of digital piracy examined in this study can be found in the Appendix.

MEASURES

Dependent measure. To stay consistent with previous research on deterrence (Pogarsky & Piquero, 2004), the dependent measure in the present study was the response to a single item; “I would go to the web site with the intention to download the CD under these circumstances.” Respondents marked their level of likelihood to perform the behavior on an 11-point scale that ranged from *not likely* (0) to *100% intention* (10). An individual’s intention of performing the act was indicated by higher scores reflecting greater intentions.

Low self-control. The present study used a 24-item composite scale from Grasmick, Tittle, Bursik, and Arneklev (1993) to measure low self-control. Respondents’ answers could range from 1= *strongly disagree* to 4= *strongly agree*. Higher scores on the scale indicated lower levels of self-control.

Extra-legal sanctions. To measure extralegal sanctions consistent with the contemporary view of deterrence, respondents were asked questions regarding social and self-disapproval. Social disapproval was based on two questions (see Grasmick & Bursick, 1990; Pogarsky, 2002). These two questions were asked in the present study: "How likely would it be that your family would find out that you went to the web site and downloaded the CD?" and "How likely would it be that your friends would find out that you went to the web site and downloaded the CD?" Respondents' answers were measured on an 11-point scale ranging from *not likely* to *100% likely*. Similar to Nagin and Pogarsky (2001), self-disapproval and its expected influence was measured by asking respondents to mark on a scale, with 1 = *strongly disagree* and 5 = *strongly agree*, the degree to which they agreed with the statement, "I would feel guilty for going to the web site to download the CD." Finally, the respondents were asked, "How morally wrong would it be if you were to go to the web site to download the CD?" This question was consistent with Bachman, Paternoster, and Ward (1992) and was measured on an 11-point scale anchored by *not wrong* and *100% wrong.*

Self-generated deterrence responses. Some researchers have contended that the use of hypothetical scenarios may not accurately reflect a person's real-world decision-making process because the scenarios are artificially articulated by the researcher (Bouffard, 2002; Piquero & Bouffard, in press). In particular, Bouffard (2002) argues that the use of hypothetical scenarios may lead to the priming of the respondents' answers and thus may create methodological problems. To remedy these problems, Bouffard (2002) suggests the use of participant-generated consequences to measure deterrence certainty and severity of a behavior. The present study utilized this contemporary view of deterrence theory within its methodology. After responding to the above extralegal sanction questions, respondents were presented with a table for them to develop their own measures of deterrence.

For the scenario (going to the web site to download the CD), respondents were asked to list five "bad things" that might occur if one were to engage in the act and, then on the corresponding side of the table, to indicate the importance (0% to 100%) of each of the "bad things" when they make the decision to perform the act. The use of self-generated responses will better capture an individual's true decision-making processes and better test deterrence theory. Additionally, Bouffard (2002) argues that the development of longer lists of "bad things" may indicate higher levels of self-control. Individuals with longer lists are viewed to have taken more time to think about the potential costs of a behavior, whereas those with low self-control ignore the long-term costs of the behavior, which is consistent with Gottfredson and Hirschi's (1990) contention. As a result, the respondents' self-generated responses will not only be used to gauge deterrence but also the individual's level of self-control.

One "bad thing" that respondents did list as a consequence of engaging in music piracy was computer viruses. Respondents that listed "virus" were coded as 1 and those that did not provide "virus" as a "bad thing" were coded as 0.

Additional control measures. The respondents were asked their age (an open-ended question), sex (1 = male, 0 = female), and race (1 = White, 2 = non-White), major (1 = business administration, 2 = justice administration, 3 = English, 4 = mathematics, and 5 = other), and their family's approximate total income in the past year (1 = $0 to $19,999, 2 = $20,000 to $29,999, 3 = $30,000 to $39,999, 4 = $40,000 to $49,999, and 5 = $50,000 or more). Consistent with Higgins et al. (2006), additional control measures were obtained by asking the respondents how many times in the past 2 weeks, the past month, and the past year they had engaged in music piracy. A scale called "previous music piracy" (1 = zero

times, 2 = 1 to 2 times, 3 = 3 to 4 times, and 5 = more than 5 times) was created to indicate the frequency of involvement in the behavior. They were also asked to indicate how many times the individual's male friends had participated in each of the activities during similar time intervals.1 Respondents marked their answers on scales ranging from zero times to more than 5 times.

RESULTS

Table 2 presents the descriptive statistics and bivariate correlations for the measures used for this study. The associations between guilt and intention to download (r = -.47), previous music piracy and intention to download (r = .40), and male friend downloading behavior and previous music piracy (r = .41) were significant and in their predicted directions. The association between moral beliefs and guilt (r = .60) was the strongest. This indicates that multicollinearity may be present in these data. Guilt (r = -.13) and male friend downloading behavior were the only measures that had significant associations with obtaining a virus from downloading a CD. These relationships were weak. However, the correlations show that the more moral beliefs increased the less likely it was for an individual to see viruses as a deterrent to committing music piracy. And when an individual's male friends' downloading behavior increased, that individual was more likely to view viruses as a deterrent to music piracy.

Table 2
Sample Descriptive Statistics and Bivariate Correlations of Measures ($n = 260$)

	Mean	*SD*	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1. Intention to download CD	4.38	3.72	1.00													
2. Feel guilty download CD	2.67	1.30	−0.47**	1.00												
3. Morally wrong to download	5.03	3.32	−0.35**	0.60**	1.00											
4. How likely family find out	2.98	3.61	0.12*	−0.03	−0.01	1.00										
5. How likely friends find out	5.47	3.65	0.26**	−0.15**	−0.02	0.47**	1.00									
6. Get virus if download CD	0.23	0.42	0.04	−0.13*	−0.10	0.01	0.07	1.00								
7. Previous music piracy	10.25	5.88	0.40**	−0.31**	−0.20**	0.12*	0.21**	0.04	1.00							
8. Self-control	50.34	9.37	0.23**	−0.13*	−0.13*	0.11	0.16**	−0.03	0.06	1.00						
9. Male friends download	7.90	3.26	0.33**	−0.33**	−0.28**	0.10	0.26**	0.12*	0.41**	0.17**	1.00					
10. Sex	0.40	0.49	0.05	−0.14*	−0.13*	−0.18**	−0.09	0.01	0.14*	0.10	0.13*	1.00				
11. Age	4.35	2.76	−0.13*	0.09	0.04	0.03	−0.17**	0.06	−0.20**	−0.03	−0.22**	0.04	1.00			
12. Major	4.03	1.46	−0.03	0.09	0.04	0.00	−0.01	−0.05	−0.11*	−0.06	−0.06	−0.09	−0.03	1.00		
13. Race	1.30	0.61	0.10	−0.05	−0.06	0.05	0.05	0.03	−0.03	−0.10	−0.01	−0.02	−0.06	0.01	1.00	
14. Income	3.78	1.45	0.01	−0.01	0.04	0.07	0.12*	0.00	0.17**	0.05	0.13*	0.10	−0.26**	−0.12*	−0.17**	1.00

* Statistical significance at the .05 level.
** Statistical significance at the .01 level.

Table 3 presents results from the ordinary least squares (OLS) regression analysis that applied contemporary deterrence measures to point to strategies to reduce music piracy. This model allows us to examine the additive links between the independent measures and music piracy. Specifically, an individual's previous music piracy (*b* = .15, *B* = .24, *t* = 3.86) had a positive link to music piracy. This indicates that individuals that have experience with the intentions to pirate music are likely to pirate music. Low self-control has a link with intentions to pirate music (*b* = .05, *B* = .13, *t* = 2.46). This indicates support for Gottfredson and Hirschi's (1990) contention that individuals with lower levels of self-control are likely to engage or intend to engage in criminal and deviant behavior.

Table 3
Multiple Regression With Intention to Download CD as the Dependent Variable ($n = 260$)

	b	*SE*	Beta	Tolerance	VIF
1. Feel guilty	−.90**	.20	−.31	.55	1.83
2. How likely family find out	−.02	.06	−.02	.71	1.41
3. How likely friends find out	.12	.06	.12	.68	1.48
4. How morally wrong	−.04	.07	−.04	.61	1.63
5. Previous music piracy	.15**	.04	.24	.70	1.43
6. Self-control	.05**	.02	.13	.91	1.10
7. Male friends download	.05	.07	.04	.66	1.51
8. Attitudes toward downloading	.08	.05	.10	.72	1.39
9. Sex	−.33	.41	−.04	.86	1.16
10. Age	.01	.08	.01	.77	1.30
11. Major	−.05	.13	−.02	.95	1.06
12. Race	.59	.43	.07	.92	1.08
13. Income	−.26	.14	−.10	.85	1.17
14. Get virus if download CD	−.35	.44	−.04	.96	1.04
f	10.07**				
R^2	.36				
Adjusted R^2	.33				

Note: VIF = variance inflation factor.
** Statistical significance at the .01 level.

Feeling guilty about music piracy (*b* = -.90, *B* = -.31, *t* = -4.55) had the strongest association of the model with a negative relationship with music piracy. These results suggest that individuals are capable of feeling guilt when intending to pirate music. This is a finding consistent with Higgins et al. (2006). Results from the regression showed that the three measures accounted for 36% of the variance in music piracy. None of the demographic measures (i.e., sex, age, major, race, or income) were shown to have any statistically significant associations with music piracy.

Table 4
Multiple Regression With Intention to Download CD as the Dependent Variable by Yes/No to Get Virus if Download CD

	Yes—Get Virus ($n = 65$)					No—Get Virus ($n = 195$)					
	b	*SE*	Beta	Tol.	VIF	*b*	*SE*	Beta	Tol.	VIF	*z*
1. Feel guilty	−1.32**	0.45	−.45	.49	2.03	−0.81**	.23	−.28	.54	1.85	−1.01
2. How likely family find out	0.00	0.14	.00	.69	1.45	−0.03	.07	−.03	.65	1.54	
3. How likely friends find out	0.15	0.14	.15	.67	1.50	0.10	.07	.10	.65	1.53	
4. How morally wrong	0.03	0.17	.03	.53	1.89	−0.04	.08	−.04	.59	1.69	
5. Previous music piracy	0.11	0.09	.17	.53	1.88	0.16**	.04	.25	.69	1.46	−0.51
6. Male friends download	−0.07	0.19	−.06	.51	1.96	0.09	.08	.08	.66	1.51	
7. Attitudes toward download	0.03	0.18	.02	.66	1.51	0.09	.05	.12	.69	1.46	
8. Self-control	0.05	0.06	.11	.73	1.36	0.05*	.02	.14	.89	1.13	0.00
9. Sex	0.00	0.98	.00	.76	1.31	−0.41	.48	−.06	.84	1.19	
10. Age	−0.12	0.17	−.09	.73	1.37	0.05	.09	.04	.75	1.34	
11. Major	0.12	0.33	.05	.70	1.43	−0.06	.15	−.02	.91	1.10	
12. Race	0.00	1.09	.00	.75	1.34	0.75	.50	.09	.90	1.11	
13. Income	−0.54	0.31	−.21	.85	1.18	−0.16	.17	−.06	.79	1.26	
f	2.60**					8.17**					
R^2	0.40					0.37					
Adjusted R^2	0.25					0.32					

Note: VIF= variance inflation factor; Tol. = tolerance.
* Statistical significance at the .05 level.
** Statistical significance at the .01 level.

Multicollinearity was suggested to have been a possible problem in the bivariate correlation analysis. However, results from tolerance coefficients and variance inflation factors (VIFs) within OLS show that multicollinearity was not an issue with the measures. Field (2000) argued that tolerance coefficients below .20 and VIFs above 4 are problematic. The analyses in Table 3 show that these standards for tolerance and VIF were not met, meaning that multicollinearity was not an issue for this study.

Table 4 presents results from multiple regression analyses that were split by an individual's indication of whether a virus is a "bad thing." This allows us to examine a possible interaction between the perception of getting a virus and the other independent measures because they may link with music piracy.2We used intention to download a CD illegally as the dependent variable. To probe the statistically significant coefficients across the two groups, we used the Paternoster, Brame, Mazerolle, and Piquero (1998) *z*-score. In the "no viruses" group, self-control (*b* = .05, *B* = .14, *z* = .00) and previous music piracy (*b* = .16, *B* = .25, *z* = -.51) were shown to have positive associations with an individual's likelihood of seeing computer viruses as a potential consequence of engaging in music piracy. As an individual's level of self-control decreased or his or her previous music piracy frequency increased, the individuals were more likely to intend to pirate music. The self-control findings are consistent with Gottfredson and Hirschi's (1990) theory in that those with low self-control are likely to pirate music because they do not see viruses as a deterrent.

In the context of deterrence theory in the "no virus" group, the only measure that was statistically significant was guilt (*b* = -.81, *B* = -.28, *z* = -1.01). When comparing guilt to low self-control and to prior music piracy, guilt has the strongest association in the entire model. This suggests that individuals who do not see viruses as a deterrent see guilt as a deterrent, and the *z*-score is larger than the effect of the individual propensities (i.e., self-control). For the "yes virus" group, "feeling guilty" (*b* = -1.32, *B* = -.45, *z* = -1.01) was the only significant measure from the model. As an individual's level of guilt increased, the likelihood of him or her listing viruses as a consequence decreases. This is in contrast to the "no virus" model that showed individual propensities (i.e., self-control) were statistically significant and relevant in producing intentions to pirate music. That is, for individuals that listed "no virus," the individuals' level of self-control did not cloud their view of the consequences of their actions regarding music piracy. Thus, the perception of downloading a virus may be considered a deterrent for digital piracy.3

The analysis turns to multicollinearity. As with Table 3, the tolerance and VIF are within their standard, which indicates that multicollinearity is not a problem. Thus, we interpret these findings as free from multicollinearity.

DISCUSSION

The findings from the present study indicate that deterrence is important in understanding factors for reducing instances of digital piracy (Paternoster, 1987; Yu & Liska, 1993). The findings suggest that guilt is an important factor in reducing instances of digital piracy (Higgins et al., 2006). Furthermore, the findings support previous research that low selfcontrol has a link with digital piracy (Higgins, 2005; Higgins et al., 2005; Higgins et al., 2006). The uniqueness of the present study comes in its inclusion of computer viruses as a selfgenerated
deterrent for digital piracy. The use of viruses in this study was compared against the other deterrent measures and low self-control. The results from the main analysis do not

show that viruses are an important deterrent factor for reducing instances of digital piracy. This is not in accord with the view from the IFPI (2006).

The role of viruses as a deterrent was probed by splitting the sample for those that did say that viruses were a deterrent and those that did not say that viruses were a deterrent. This analysis takes into account that viruses do have an effect on the measures, but the effect is masked by the other measures. For those who do not see viruses as an important deterrent, low self-control (Higgins et al., 2006) and guilt (Higgins et al., 2006) are important measures. However, those that see viruses as an important deterrent also see guilt as a deterrent. Importantly, for these individuals, the propensities to digital piracy are not significant. This finding suggests that viruses are a deterrent, supporting the view from the IFPI. Thus, individuals who perceive that they will download a virus are less likely to digitally pirate. This is indicated by removing the positive effects of all other measures but leaving the negative effect of guilt.

The findings from this study suggest avenues for reducing instances of digital piracy. For example, policy makers can use guilt to reduce instances of digital piracy. This may be accomplished by placing statements in downloading procedures that incite guilt. Furthermore, this preliminary study indicates that the ethical use of viruses may be important in reducing instances of digital piracy. That is, security administrators may be able to ethically attach a virus to downloadable music files or within peer-to-peer formats so that the viruses are attached to those files when downloaded.

Although the findings of this study suggest that guilt and viruses may be important in reducing instances of digital piracy, the findings have limits. That is, our measurement of viruses is not a direct measure afforded to all individuals. Although our measurement may not be standardized for all individuals, this strategy is relevant because it follows the more contemporary method prescribed by Bouffard (2002) for gathering deterrence information. In addition, our split sample analysis may be biased because of the small sample size. However, we performed a simulation analysis that illustrates very little bias and proper power levels for the analysis. Furthermore, the analysis only comes from one college. Additional studies in this area that use larger sample sizes are warranted to further understand this connection.

Despite the limits of the present study, deterrence is an important perspective in understanding the measures that can be used to reduce instances of digital piracy. Studies that address the standardization of the measurement, the small sample size, and the generalizability of the findings would be important in our understanding of reducing digital piracy. Our findings indicate that guilt and viruses may be used to reduce instances of digital piracy.

APPENDIX

Scenario 1

A popular CD has just been released to music stores nationwide. All of your friends have heard the CD and told you that it is great and that you have to get it! Unfortunately, every time that you try to go to get the CD, you cannot because it is always sold out. However, a friend tells you about an underground online web site that has posted an underground copy of the entire CD. The site will only allow visitors to download the CD before the visitors can listen to it. You really want the CD.

NOTES

1. Substantively, the results are the same with or without the inclusion of female friends' downloading behavior. The study only uses male friends' downloading behavior in the analysis for this reason.
2. Furthermore, following the suggestions of an anonymous reviewer, we performed a mean difference analysis that showed "Get Virus" did have a significant effect on the intentions to perform digital piracy. Therefore, we are able to conclude that getting a virus had a mean effect on intentions to perform digital piracy.
3. We performed a regression analysis that took into account the interaction between feeling guilty and getting a virus, previous music piracy and getting a virus, and self-control and getting a virus. Our results were substantively the same as in the split regression analysis. We would like to thank the anonymous reviewers for this suggestion because of concerns about statistical power.

REFERENCES

Akers, R. L. (1998). *Social learning and social structure: A general theory of crime and deviance.* Boston: Northeastern University Press.

Bachman, R., Paternoster, R., & Ward, S. (1992). The rationality of sexual offending: Testing a deterrence/rational choice conception of sexual assault. *Law and Society Review, 26,* 343-372.

Balthrop, J., Forrest, S., Newman, M. E. J., & Williamson, M. M. (2004). Technological networks and the spread of computer viruses. *Science, 304*, 527-529.

Bouffard, J. A. (2002). Methodological and theoretical implications of using subject-generated consequences in tests of rational choice theory. *Justice Quarterly, 19,* 747-771.

Chiou, J. S., Huang, C., & Lee, H. (2005). The antecedents of music piracy attitudes and intentions. *Journal of Business Ethics, 57,* 161-174.

Christensen, A., & Eining, M. M. (1991). Factors influencing software piracy: Implications for accountants. *Journal of Information Systems, 5,* 67-80.

Cochran, J. K.,Wood, P. B., Sellers, C. S.,Wilkerson,W., & Chamlin, M. B. (1998). Academic dishonesty and low self-control: An empirical test of a general theory of crime. *Deviant Behavior, 19,* 227-255.

d'Astous, A., Colbert, F., & Montpetit, D. (2005). Music piracy on the web—How effective are anti-piracy arguments? Evidence from the theory of planned behaviour. *Journal of Consumer Policy, 28,* 289-310.

Easley, R. F., Michel, J. G., & Devaraj, S. (2003). The MP3 open standard and the music industry's response to Internet piracy. *Association for Computing Machinery, 46,* 90-98.

Field, A. (2000). *Discovering statistics using SPSS for windows.* Thousand Oaks, CA: Sage.
Fivelsdal, H. (2005). Moving toward a balanced and effective response to internet music piracy. *The International Journal of Media Management, 7,* 121-126.

Gopal, R., & Sanders, G. L. (1997). Preventive and deterrent controls for software piracy. *Journal of Management Information Systems, 13,* 29-47.

Gopal, R., Sanders, G. L., Bhattacharjee, S., Agrawal, M., & Wagner, S. (2004). A behavioral model of digital music piracy. *Journal of Organizational Computing and Electronic Commerce, 14,* 89-105.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford, CA: Stanford University Press. Grasmick, H. G., & Bursik, R. J. (1990). Conscience, significant others, and rational choice: Extending the deterrence model. *Law & Society Review, 24,* 837-861.

Grasmick, H. G., Tittle, C. R., Bursik, R. J., & Arneklev, B. J. (1993). Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime. *Journal of Research in Crime and Delinquency*, *30,* 5-29.

Harmer, P. K., Williams, P. D., Gunsch, G. H., & Lamont, G. B. (2002). An artificial immune system architecture for computer security applications. *IEEE Transactions on Evolutionary Computation, 6*, 252-280.

Higgins, G. E. (2005). Can self-control theory help understand the software piracy problem? *Deviant Behavior, 26,* 1-24.

Higgins, G. E., Fell, B. D., & Wilson, A. L. (2006). Digital piracy: Assessing the contributions of an integrated self-control theory and social learning theory using structural equation modeling. *Criminal Justice Studies: A Critical Journal of Crime, Law, & Society, 19,* 3-22.

Higgins, G. E., & Makin, D. A. (2004a). Does social learning theory condition the effects of low self-control on college students' software piracy? *Journal of Economic Crime Management, 2,* 1-22.

Higgins, G. E., & Makin, D. A. (2004b). Self-control, deviant peers, and software piracy. *Psychological Reports, 95,* 921-931.

Higgins, G. E., Wilson, A. L., & Fell, B. D. (2005). An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture, 12,* 166-194.

Hinduja, S. (2001). Correlates of internet software piracy. *Journal of Contemporary Criminal Justice, 17,* 369-382.

Hinduja, S. (2003). Trends and patterns among online software pirates. *Ethics and Information Technology, 5,* 49-61.

Hollinger, R. C. (1988). Computer hackers follow a Guttman-like progression. *Sociology and Social Research, 72,* 199-200.

Husted, B. W. (2000). The impact of national culture on software piracy. *Journal of Business Ethics, 13,* 431-438.

International Federation of Phonographic Industries (IFPI). (2006). *The recording industry 2006 piracy report: Protecting creativity in music.* Retrieved December 7, 2006, from http://www.ifpi.org

Klepper, S., & Nagin, D. (1989). The deterrent effect of perceived certainty and severity of punishment revisited. *Criminology, 27,* 721-746.

Koen, C. M., & Im, J. H. (1997). Software piracy and its legal implications. *Security Journal*, *31,* 265-272.

Liang, Z., & Yan, Z. (2005). Software piracy among college students: A comprehensive review of contributing factors, underlying processes, and tackling strategies. *Journal of Educational Computing Research, 33,* 115-140.

Lloyd, A. L., & May, R. M. (2001). How viruses spread among computers and people. *Science, 292*, 1316-1317. Love, S. R. (2006). Illicit sexual behavior: A test of self-control theory. *Deviant Behavior, 27,* 505-536.

Nagin, D. S. (1998). Deterrence and incapacitation. In M. H. Tonry (Ed.), *Handbook of crime and punishment* (pp. 345-368). Oxford, United Kingdom: Oxford University Press.

Nagin, D. S., & Paternoster, G. (1991). The preventive effects of the perceived risk of arrest: Testing an expanded conception of deterrence. *Criminology, 29,* 561-587.

Nagin, D. S., & Paternoster, G. (1993). Enduring individual differences and rational choice theories of crime. *Law & Society Review, 27,* 467-496.

Nagin, D. S., & Pogarsky, G. (2001). Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence. *Criminology, 39,* 865-892.

Nagin, D. S., & Pogarsky, G. (2003). An experimental investigation of deterrence: Cheating, self-serving bias, and impulsivity. *Criminology, 41,* 167-193.

Nagin, D. S., & Pogarsky, G. (2004). Time and punishment: Delayed consequences and criminal behavior. *Journal of Quantitative Criminology, 20,* 295-318.

Paternoster, R. (1986). The use of composite scales in perceptual deterrence research: A cautionary note. *Journal of Research in Crime and Delinquency, 23,* 128-169.

Paternoster, R. (1987). The deterrent effect of the perceived certainty and severity of punishment: A review of the evidence and issues. *Justice Quarterly*, *4,* 173-217.

Paternoster, R., Brame, R., Mazerolle, P., & Piquero, A. (1998). Using the correct statistical test for the equality of regression coefficients. *Criminology, 36,* 859-866.

Paternoster, R., & Piquero, A. (1995). Reconceptualizing deterrence: An empirical test of personal and vicarious experiences. *Journal of Research in Crime and Delinquency, 32,* 251-286.

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review, 30,* 549-583.

Peace, A. G., Galletta, D. F., & Thong, J. Y. L. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems, 20,* 153-177.

Piquero, A. R., & Bouffard, J. A. (In press). Something old, something new: A preliminary investigation of Hirschi's redefined self-control. *Justice Quarterly.*

Piquero, A. R., & Pogarsky, G. (2002). Beyond Stafford and Warr's reconceptualization of deterrence: Personal and vicarious experiences, impulsivity, and offending behavior. *Journal of Research in Crime and Delinquency, 39,* 153-187.

Piquero, A. R., & Tibbetts, S. (1996). Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending. *Justice Quarterly, 13,* 481-510.

Pogarsky, G. (2002). Identifying "deterrable" offenders: Implications for research on deterrence. *Justice Quarterly, 19,* 431-453.

Pogarsky, G. (2004). Projected offending and contemporaneous rule-violation. *Criminology, 42,* 111-136.

Pogarsky, G., & Piquero, A. R. (2004). Studying the reach of deterrence: Can deterrence theory help explain police misconduct? *Journal of Criminal Justice, 32,* 371-386.

Sherizen, S. (1995). Can computer crime be deterred? *Security Journal, 6,* 177-181.

Skinner,W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency, 34,* 495-518.

Sutherland, E. D. (1947). *Principles of criminology* (4th ed.). Philadelphia, PA: J.B. Lippincott.
Tibbetts, S. G. (1997). Shame and rational choice in offending decisions. *Criminal Justice and Behavior, 24,* 234-255.

Tibbetts, S. G., & Myers, D. L. (1999). Low self-control, rational choice, and student test cheating. *American Journal of Criminal Justice, 23,* 179-200.

Tyler, T. R., & Huo,Y. J. (2002). *Trust in the law: Encouraging public cooperation with the police and courts.* New York: Russell Sage.

Wade, J. (2004). The music industry's war on piracy. *Risk Management, 51,* 10-16.

Wagner, S. C., & Sanders, G. L. (2001). Considerations in ethical decision-making and software piracy. *Journal of Business Ethics, 29,* 161-167.

Wall, D. S. (2005). The Internet as a conduit for criminal activity. In A. Pattavina (Ed.), *Information technology and the criminal justice system* (pp. 78-94). Thousand Oaks, CA: Sage.

Wright, B. R. E., Caspi, A., Moffitt, T. E., & Paternoster, R. (2004). Does the perceived risk of punishment deter criminally prone individuals? Rational choice, self-control, and crime. *Journal of Research in Crime and Delinquency, 31,* 447-464.

Yu, J., & Liska, A. (1993). The certainty of punishment: A reference group effect and its functional form. *Criminology*, *31,* 447-464.